Plugging the WikiLeak: What can the government do?

August 7 2010, By LOLITA C. BALDOR , Associated Press Writer

In this Sunday Aug. 1, 2010, photo released by CBS, Adm. Michael Mullen, Chairman of the Joint Chiefs of Staff, discusses the war in Afghanistan on CBS's "Face The Nation" in Washington. Mullen said the Pentagon is trying to protect Afghans who may be at risk from Taliban retaliation following the publication of tens of thousands of secret war documents, posted on the website WikiLeaks a week ago. He said the U.S. is duty-bound to try to shield informants who were named in the documents. (AP Photo/CBS, Chris Usher) NO ARCHIVES. NO SALES.

(AP) -- An online whistle-blower's threat to release more classified Pentagon and State Department documents is raising difficult questions of what the government can or would do, legally, technically or even militarily to stop it.

Constrained by the global reach of the Internet, sophisticated encryption

software and the domestic legal system, the answer seems to be: Not much.

But if the U.S. government believes that the release of classified documents WikiLeaks is preparing to disclose will threaten national security or put lives at risk, cyber and legal experts say the options could expand to include cyber strikes to take down the WikiLeaks website and destroy its files or covert operations to steal or disable the files.

It all sounds, at times, like a spy movie, where the possibilities extend as far as the imagination can reach. But most outsiders agree that reality is probably far less dramatic.

At the center of the drama was the posting last week of a massive 1.4 gigabyte mystery file named "Insurance" on the WikiLeaks website.

The "Insurance" file is encrypted, nearly impossible to open until WikiLeaks provides the passwords. But experts suggest that if anyone can crack it - it would be the National Security Agency.

That file, coupled with WikiLeaks' release of more than 77,000 secret military documents last month, prompted the Pentagon to demand that the website's editor-in-chief, Julian Assange, cancel any new document dumps and pull back the Afghan war data he already posted.

WikiLeaks slammed the demand as an obnoxious threat, and Pentagon spokesman Geoff Morrell declined to detail what, if any, actions the Defense Department may be ready to take.

Few people involved, for the Pentagon and other agencies, would talk openly about what the Pentagon or the clandestine NSA could or would do to stop the expected document dump. It is not even clear if U.S. officials actually know what WikiLeaks has.

"Do we believe that WikiLeaks has additional cables? We do," said State Department spokesman P.J. Crowley. "Do we believe that those cables are classified? We do. And are they State Department cables? Yes."

Officials say the data may also include up to 15,000 military documents related to the Afghanistan war that were not made public in the initial release.

Assuming the documents contain highly sensitive information that threatens national security, the U.S. must weigh a number of options, experts say.

First, from a legal standpoint, there is probably little the U.S. government can do to stop WikiLeaks from posting the files.

It is against federal law to knowingly and willfully disclose or transmit classified information. But Assange, an Australian who has no permanent address and travels frequently, is not a U.S. citizen.

Since Assange is a foreign citizen living in a foreign country, it's not clear that U.S. law would apply, said Marc Zwillinger, a Washington lawyer and former federal cyber crimes prosecutor. He said prosecutors would have to figure out what crime to charge Assange with, and then face the daunting task of trying to indict him or persuade other authorities to extradite him.

It would be equally difficult, Zwillinger said, to effectively use an injunction to prevent access to the data.

"Could the U.S. get an injunction to force U.S. Internet providers to block traffic to and from WikiLeaks such that people couldn't access the website?" Zwillinger said. "It's an irrelevant question. There would be thousands of paths to get to it. So it wouldn't really stop people from

getting to the site. They would be pushing the legal envelope without any real benefit."

Legal questions aside, the encrypted file conjures visions of secret codebreakers hunched over their laptops, tearing open secret, protected files in seconds with a few keystrokes.

Reality is not that simple. It appears WikiLeaks used state-of-the-art software requiring a sophisticated electronic sequence of numbers, called a 256-bit key, to open them.

The main way to break such an encrypted file is by what's called a "brute force attack," which means trying every possible key, or password, said Herbert Lin, a senior computer science and cryptology expert at the National Research Council of the National Academy of Sciences.

Unlike a regular six- or eight-character password that most people use every day, a 256-bit key would equal a 40 to 50 character password, he said.

If it takes 0.1 nanosecond to test one possible key and you had 100 billion computers to test the possible number variations, "it would take this massive array of computers 10 to the 56th power seconds - the number 1, followed by 56 zeros" to plow through all the possibilities, said Lin.

How long is that?

"The age of the universe is 10 to the 17th power seconds," explained Lin. "We will wait a long time for the U.S. government or anyone else to decrypt that file by brute force."

Could the NSA, which is known for its supercomputing and massive

electronic eavesdropping abilities abroad, crack such an impregnable code?

It depends on how much time and effort they want to put into it, said James Bamford, who has written two books on the NSA.

The NSA has the largest collection of supercomputers in the world. And officials have known for some time that WikiLeaks has classified files in its possession.

The agency, he speculated, has probably been looking for a vulnerability or gap in the code, or a backdoor into the commercial encryption program protecting the file.

At the more extreme end, the NSA, the Pentagon and other U.S. government agencies - including the newly created Cyber Command - have probably reviewed options for using a cyber attack against the website, which could disrupt networks, files, electricity, and so on.

"This is the kind of thing that they are geared for," said Bamford, "since this is the type of thing a terrorist organization might have - a website that has damaging information on it. They would want to break into it, see what's there and then try to destroy it."

The vast nature of the Internet, however, makes it essentially impossible to stop something, or take it down, once it has gone out over multiple servers.

In the end, U.S. officials will have to weigh whether a more aggressive response is worth the public outrage it would likely bring. Most experts predict that, despite the uproar, the government will probably do little other than bluster, and the documents will come out anyway.

"Once you start messing with the Internet, taking things down, and going to the maximum extent to hide everything from coming out, it doesn't necessarily serve your purpose," said Bamford. "It makes the story bigger than it would have been had the documents been released in the first place."

"If, in the end, the goal is to decrease the damage, you have to wonder whether pouring fuel on the fire is a reasonable solution," he said.

More information: Online:www.wikileaks.org/